

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Xavier Boyen
Application No. :
Confirmation No. :
Filed : Herewith
For : IDENTITY-BASED SIGNCRYPTION SYSTEM
Group Art Unit :
Examiner :


Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98,
applicants hereby bring the attention of the Examiner to the
documents listed on the attached Form PTO-1449 (submitted in
duplicate).

Respectfully Submitted,


G. Victor Treyz
Reg. No. 36,294
Attorney for Applicant
Customer No. 36532

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		Complete if Known			
		Application Number			
		Filing Date	Herewith		
		First Named Inventor	Xavier Boyen		
		Art Unit			
		Examiner Name			
Sheet	1	of	1	Attorney Docket Number	ID-5

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		J.H. AN et al "On the security of join signature and encryption" in Proc. Eurocrypt '02, LNCS 2332, 2002; Cryptography ePrint Archive Report 2002/046; http://eprint.iacr.org/2002/046/ (June 17, 2002)	
		D. BONEH et al. "Identity-based encryption from the Weil pairing." Cryptography ePrint Archive Report 2001/090; http://eprint.iacr.org/2001/090/ (2001)	
		J.C. CHA et al. "An identity-based signature from the gap Diffie-Hellman groups." Cryptography ePrint Archive Report 2002/018; http://eprint.iacr.org/2002/018/ (2002)	
		F. HESS "Exponent group signature schemes and efficient identity based signature schemes based on pairings" Cryptography ePrint Archive Report 2002/012; http://eprint.iacr.org/2002/012/ (2002)	
		B. LIBERT et al. "New identity based signcryption schemes based on pairings" Cryptography ePrint Archive Report 2003/023; http://eprint.iacr.org/2003/023/ (2003)	
		B. LYNN "Authenticated identity-based encryption" Cryptography ePrint Archive Report 2002/072; http://eprint.iacr.org/2002/072/ (2002)	
		J. MALONE_LEE "Identity-based signcryption" Cryptography ePrint Archive Report 2002/098; http://eprint.iacr.org/2002/098/ (2002)	
		K.G. Paterson. "ID-based signatures from pairings on elliptic curves" Cryptography ePrint Archive Report 2002/004; http://eprint.iacr.org/2002/004/ (2002)	

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		Complete if Known			
		Application Number			
		Filing Date	Herewith		
		First Named Inventor	Xavier Boyen		
		Art Unit			
		Examiner Name			
Sheet	1	of	1	Attorney Docket Number	ID-5

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		J.H. AN et al "On the security of join signature and encryption" in Proc. Eurocrypt '02, LNCS 2332, 2002; Cryptography ePrint Archive Report 2002/046; http://eprint.iacr.org/2002/046/ (June 17, 2002)	
		D. BONEH et al. "Identity-based encryption from the Weil pairing." Cryptography ePrint Archive Report 2001/090; http://eprint.iacr.org/2001/090/ (2001)	
		J.C. CHA et al. "An identity-based signature from the gap Diffie-Hellman groups." Cryptography ePrint Archive Report 2002/018; http://eprint.iacr.org/2002/018/ (2002)	
		F. HESS "Exponent group signature schemes and efficient identity based signature schemes based on pairings" Cryptography ePrint Archive Report 2002/012; http://eprint.iacr.org/2002/012/ (2002)	
		B. LIBERT et al. "New identity based signcryption schemes based on pairings" Cryptography ePrint Archive Report 2003/023; http://eprint.iacr.org/2003/023/ (2003)	
		B. LYNN "Authenticated identity-based encryption" Cryptography ePrint Archive Report 2002/072; http://eprint.iacr.org/2002/072/ (2002)	
		J. MALONE_ LEE "Identity-based signcryption" Cryptography ePrint Archive Report 2002/098; http://eprint.iacr.org/2002/098/ (2002)	
		K.G. Paterson. "ID-based signatures from pairings on elliptic curves" Cryptography ePrint Archive Report 2002/004; http://eprint.iacr.org/2002/004/ (2002)	

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.